

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

PCT

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT(règle 92bis.1 et
instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

NONNENMACHER, Bernard
Gemplus S.C.A.
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année) 28 septembre 2000 (28.09.00)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire GEM 576	
Demande internationale no PCT/FR99/01996	Date du dépôt international (jour/mois/année) 16 août 1999 (16.08.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse

GEMPLUS S.C.A.
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☒ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

GEMPLUS
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur ☐ aux offices désignés concernés
☐ à l'administration chargée de la recherche internationale ☒ aux offices élus concernés
☒ à l'administration chargée de l'examen préliminaire international ☐ autre destinataire:
Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:

Sean Taylor

no de téléphone (41-22) 338.83.38

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 21 mars 2000 (21.03.00)	
Demande internationale no PCT/FR99/01996	Référence du dossier du déposant ou du mandataire GEM 576
Date du dépôt international (jour/mois/année) 16 août 1999 (16.08.99)	Date de priorité (jour/mois/année) 17 août 1998 (17.08.98)
Déposant CORON, Jean-Sébastien etc	

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

15 février 2000 (15.02.00)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection



a été faite



n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

R. Forax

no de téléphone: (41-22) 338.83.38

TRA DE COOPERATION EN MATIERE DE BREVETS

P.B.

Expéditeur : L'ADMINISTRATION CHARGÉE DE
LA RECHERCHE INTERNATIONALE

PCT

U

Destinataire

GEMPLUS S.C.A.
Avenue du Pic de Bertagne
A l'att. de NONNENMACHER, B.
Parc d'activités de GEMENOS
BP 100
13881 GEMENOS Cedex
FRANCE

NOTIFICATION DE TRANSMISSION DU
RAPPORT DE RECHERCHE INTERNATIONALE
OU DE LA DECLARATION

(règle 44.1 du PCT)

REÇU le
02 DEC. 1999

Date d'expédition
(jour/mois/année)

30/11/1999

Référence du dossier du déposant ou du mandataire

GEM 576

POUR SUITE A DONNER

voir les paragraphes 1 et 4 ci-après

Demande internationale n°

PCT/FR 99/01996

Date du dépôt international

(jour/mois/année)

16/08/1999

Déposant

GEMPLUS S.C.A. et al.

1. ☒ Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :

Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

Où? Directement auprès du Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. ☐ Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2(a), est transmise ci-joint.

3. ☐ En ce qui concerne la réserve pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

☐ la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

☐ la réserve n'a encore fait l'objet d'aucune décision: dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90bis.1 et 90bis.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).

Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale



Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Grace Casuga

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand?

Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment?

Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/puvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220 (suite)

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

- i) la revendication n'est pas modifiée;
- ii) la revendication est supprimée;
- iii) la revendication est nouvelle;
- iv) la revendication remplace une ou plusieurs revendications telles que déposées;
- v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."
2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
"Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."
3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."
4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendications 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)".

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 576	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/FR 99/01996	Date du dépôt international (jour/mois/année) 16/08/1999	(Date de priorité (la plus ancienne) (jour/mois/année) 17/08/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.



Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.



la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :



contenu dans la demande internationale, sous forme écrite.



déposée avec la demande internationale, sous forme déchiffrable par ordinateur.



remis ultérieurement à l'administration, sous forme écrite.



remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.



La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.



La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,



le texte est approuvé tel qu'il a été remis par le déposant.



Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,



le texte est approuvé tel qu'il a été remis par le déposant



le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des **dessins** à publier avec l'abrégé est la Figure n°



suggérée par le déposant.



parce que le déposant n'a pas suggéré de figure.



parce que cette figure caractérise mieux l'invention.



Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 99/01996

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/22

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L H03K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	SADEGHIYAN B ET AL: "A new universal test for bit strings" LECTURE NOTES IN COMPUTER SCIENCE, US, SPRINGER VERLAG, NEW YORK, NY, page 311-319-319 XP002101032 ISSN: 0302-9743 abrégé page 311, ligne 1 -page 318, ligne 10	1-9
A	MAURER U M: "A universal statistical test for random bit generators." J.CRYPTOL. (USA), JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, 1992, pages 89-105, XP002122895 cited by the applicant	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

17 novembre 1999

Date d'expédition du présent rapport de recherche internationale

30/11/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Gautier, L

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 15 NOV 2000

WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire GEM 576	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/01996	Date du dépôt international (jour/mois/année) 16/08/1999	Date de priorité (jour/mois/année) 17/08/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/22		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 9 feuilles, y compris la présente feuille de couverture.
 - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☒ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 15/02/2000	Date d'achèvement du présent rapport 13.11.2000
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Dechmann, J-L N° de téléphone +49 89 2399 8826 

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/01996

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).) :

Description, pages:

1-8 version initiale

Revendications, N°:

1-10 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/01996

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

III. Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

La question de savoir si l'objet de l'invention revendiquée semble être nouveau, impliquer une activité inventive (ne pas être évident) ou être susceptible d'application industrielle n'a pas été examinée pour ce qui concerne :

- ☐ l'ensemble de la demande internationale.
- ☒ les revendications n°s 7-10.

parce que :

- ☐ la demande internationale, ou les revendications n°s en question, se rapportent à l'objet suivant, à l'égard duquel l'administration chargée de l'examen préliminaire international n'est pas tenue d'effectuer un examen préliminaire international (*préciser*) :
- ☒ la description, les revendications ou les dessins (*en indiquer les éléments ci-dessous*), ou les revendications n°s 7-10 en question ne sont pas claires, de sorte qu'il n'est pas possible de formuler une opinion valable (*préciser*) :
voir feuille séparée
- ☐ les revendications, ou les revendications n°s en question, ne se fondent pas de façon adéquate sur la description, de sorte qu'il n'est pas possible de formuler une opinion valable.
- ☐ il n'a pas été établi de rapport de recherche internationale pour les revendications n°s en question.
2. Le listage des séquences de nucléotides ou d'acides aminés n'est pas conforme à la norme prévue dans l'annexe C des instructions administratives, de sorte qu'il n'est pas possible d'effectuer un examen préliminaire international significatif:
- ☐ le listage présenté par écrit n'a pas été fourni ou n'est pas conforme à la norme.
- ☐ le listage sous forme déchiffrable par ordinateur n'a pas été fourni ou n'est pas conforme à la norme.

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/01996

1. Déclaration

Nouveauté	Oui : Revendications 2-6
	Non : Revendications 1
Activité inventive	Oui : Revendications 4
	Non : Revendications 1-3,5-6
Possibilité d'application industrielle	Oui : Revendications 1-6
	Non : Revendications

**2. Citations et explications
voir feuille séparée**

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

III. Non-Formulation d'opinion quant à la nouveauté, l'activité inventive et l'application industrielle

Eu égard aux différents problèmes de clarté (voir section VIII), il n'a pas été possible de formuler une opinion valable quant à la nouveauté et à l'activité inventive pour les revendications de dispositif 7 à 10.

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

I

Les documents (D) suivants ont été pris en compte pour l'établissement du rapport d'examen préliminaire:

- D1: LECTURE NOTES IN COMPUTER SCIENCE, page 311-319, SADEGHIYAN B ET AL: "A new universal test for bit strings", XP002101032
- D2: JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, 1992, pages 89-105, MAURER U M: "A universal statistical test for random bit generators", J.CRYPTOL. (USA), XP002122895

II

1. Le procédé de test de source de nombre aléatoire est revendiqué de manière trop générale de sorte qu'aucune distinction ne peut être vue entre l'objet de la revendication 1 et le contenu du document D2.

En effet comme déjà analysé dans la description par le Demandeur lui-même, la présente invention a pour but d'améliorer le procédé de test de Maurer, ou test

universel, décrit dans le document D2.

En particulier, l'invention consiste à remplacer l'étape 4 du test universel par le calcul précis de la fonction $c(L,K)$.

Cependant la formulation actuelle de la revendication indépendante de procédé 1 ne mentionne qu'un "**Calcul de la fonction $c(L,K)$** " sans donner aucun détail sur la réalisation de ce calcul. En d'autres termes l'étendue de la protection n'est pas limitée à un type de calcul particulier et comprend aussi, par exemple, le calcul selon D2. En effet, c'est seulement au niveau de la revendication 4 que sont revendiquées les étapes de calcul de la fonction $c(L,K)$ selon l'invention.

En conséquence, il est considéré que l'invention, telle qu'actuellement revendiquée dans la revendication 1, est déjà divulguée par le document D2.

Il n'est pas jugé nécessaire à ce stade de la procédure de s'étendre plus sur l'analyse du Document D2, car l'analyse de l'Examineur correspond en fait à l'analyse du Demandeur telle qu'exposée page 4 de la description.

L'objet de la revendication 1 n'est, pour cette raison, pas nouveau et la revendication 1 ne satisfait donc pas les exigences de l'Article 33(2) PCT.

2. La revendication 4 devra donc être combinée avec la revendication indépendante de procédé 1 (voir aussi section VIII).

En effet aucun des documents cités ne prévoit de remplacer l'étape 4 du test universel par un calcul plus précis de la fonction $c(L,K)$ basé sur une analyse probabiliste du test universel. Ce procédé permet d'atteindre la précision garantie par l'analyse théorique du test universel et sert notamment à améliorer la sécurité de dispositifs portables du type carte à puce.

Une telle solution implique une activité inventive et la revendication 4 satisfait donc aux exigences de l'Article 33(3) PCT

VII. Irrégularités dans la demande internationale

1. En vue de remplir les conditions de la Règle 6.3(b) PCT, les revendications

indépendantes devraient être **correctement** présentées en deux parties, les caractéristiques qui, combinées, sont comprises dans l'état de la technique (voir document D2 cité dans la section V) étant indiquées dans la première partie.

2. En vue de remplir les conditions énoncées à la Règle 5.1(a)(iii) PCT, la partie introductive de la description devra être mise en conformité avec les nouvelles revendications proposées par le Demandeur.

VIII. Observations relatives à la demande internationale

1. La **revendication de procédé 1** n'est pas claire en ce qu'elle ne contient pas toutes les caractéristiques techniques essentielles nécessaires à la définition de l'invention, conformément aux exigences de l'Article 6 pris en combinaison avec la Règle 6.3(b) PCT.

En effet la revendication 1 ne précise pas comment la quatrième étape, c.-à-d. le calcul de la fonction $c(L,K)$, est réalisée.

Cette caractéristique est cependant essentielle, car comme déjà reconnu par le Demandeur lui-même dans la description, le procédé consiste en fait à remplacer l'étape 4 du test universel par le calcul précis de la fonction $c(L,K)$ (voir page 4 de la description).

Cette caractéristique pourra être tirée de la revendication dépendante 4.

- 2a. La **revendication 7** doit être considérée comme une revendication indépendante.

En effet, une revendication peut comporter une référence à une autre revendication sans pour cela être une revendication dépendante (voir Directives PCT, C-III-3.7a).

En particulier une revendication se référant à une revendication d'une autre

catégorie (comme par exemple une revendication de dispositif se référant à une revendication de procédé) est par définition une revendication indépendante (voir Directives PCT, même paragraphe).

Cependant, le fait qu'une revendication de dispositif fasse référence à la revendication de procédé veut simplement dire que le dispositif convient pour la mise en oeuvre dudit procédé, sans pour cela définir **les moyens** qui sont pour cela nécessaires (voir aussi Directives PCT, C-III-4.8).

En fait, la revendication 7 devrait contenir explicitement, même si la référence à la revendication de procédé est maintenue, toutes les caractéristiques techniques essentielles nécessaires à la définition de l'invention (Article 6 en combinaison avec la Règle 6.3(b) PCT) et ne pas essayer, à l'aide d'un renvoi à la revendication de procédé, de les remplacer.

Par principe, en effet, une revendication indépendante doit être compréhensible par elle-même sans avoir besoin de se référer à une autre revendication.

- 2b. Il semble cependant important de mentionner à ce stade de la procédure que la description ne décrit pas un seul exemple de réalisation d'un dispositif et ne contient aucune figure décrivant une telle réalisation.
- La revendication 7 reprend quasi expressis verbis la formulation de la description qui ne contient aucun détail supplémentaire.
- Il semble donc impossible de clarifier la revendication de dispositif à l'aide de caractéristiques structurelles comprises dans la description car celle-ci n'en contient aucune. Il semble donc que la demande, concernant le dispositif, n'est pas exposée de façon suffisamment claire et complète, pour qu'un homme du métier puisse l'exécuter (Article 5 du PCT).
- 3a. Les mêmes objections de clarté concernant la revendication 7, s'appliquent à la **revendication 10**. En effet celle-ci revendique un dispositif selon les l'une des revendications 1 à 6. Cependant les revendications 1 à 6 ne sont pas des revendications de dispositif mais de procédé (problème de catégorie). Le

Demandeur veut-il dire un dispositif pour **mettre en oeuvre un procédé selon** les revendications 1 à 6. Si c'est le cas, le Demandeur n'a défini aucune caractéristique structurelle d'un tel dispositif (caractéristiques essentielles manquantes). De plus aucune caractéristiques structurelles ne sont décrites dans la description de telle sorte qu'une clarification paraît impossible (Article 5 PCT).

- 3b. De plus deux autre problèmes de clarté interviennent dans la revendication 10. Premièrement la revendication 10 fait référence aux revendications 1 à 6 qui ne contiennent aucunes références à un dispositif portable. La revendication 10 parle cependant **desdits** dispositifs portables. Deuxièmement le dispositif est un dispositif d'**auto**-vérification, auto-vérifiant son générateur aléatoire. Si ce dispositif d'**auto**-vérification est déjà sur un dispositif portable, alors que vient vérifier le dispositif extérieur? Encore une fois, la description ne vient apporter aucun éclaircissement supplémentaire car les revendications reprennent mot pour mot le peu qui est décrit à propos du dispositif dans la description.
4. En conclusion, vu les graves problèmes de clarté, il est suggéré d'abandonner toutes les revendications de dispositif et de ne conserver que les revendications de procédé en combinant les caractéristiques de la revendication 1 avec celle de la revendication 4.

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 576	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR99/01996	International filing date (day/month/year) 16 August 1999 (16.08.99)	Priority date (day/month/year) 17 August 1998 (17.08.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/22		
Applicant GEMPLUS		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>9</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p>
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input checked="" type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input checked="" type="checkbox"/> Certain observations on the international application</p>

Date of submission of the demand 15 February 2000 (15.02.00)	Date of completion of this report 13 November 2000 (13.11.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/01996

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages _____ 1-8 _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages _____ 1-10 _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/01996

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
- ☒ claims Nos. 7-10

because:

- ☐ the said international application, or the said claims Nos. _____
relate to the following subject matter which does not require an international preliminary examination (*specify*):

- ☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 7-10
are so unclear that no meaningful opinion could be formed (*specify*):

See Supplemental Box

- ☐ the claims, or said claims Nos. _____ are so inadequately supported
by the description that no meaningful opinion could be formed.
- ☐ no international search report has been established for said claims Nos. _____

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

- ☐ the written form has not been furnished or does not comply with the standard.
- ☐ the computer readable form has not been furnished or does not comply with the standard.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/01996

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III

Given the different clarity problems (see Box VIII) a valid opinion could not be drafted concerning the inventive step of device Claims 7-10.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 99/01996

V. Reasoned statement under Article 35(2) with regard to novelty; inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	2-6	YES
	Claims	1	NO
Inventive step (IS)	Claims	4	YES
	Claims	1-3, 5-6	NO
Industrial applicability (IA)	Claims	1-6	YES
	Claims		NO

2. Citations and explanations

The following documents have been considered in the drafting of the preliminary examination report:

D1: LECTURE NOTES IN COMPUTER SCIENCE, page 311-319, SADEGHIYAN B ET AL.: "A new universal test for bit strings", XP002101032

D2: JOURNAL OF CRYPTOLOGY, 1992, USA, volume 5, no. 2, 1992, pages 89-105, MAURER U M: "A universal statistical test for random bit generators", J.CRYPTOL. (USA), XP002122895

1. The method for testing a random number source is claimed in too general a manner, such that no distinction can be made between the subject matter of Claim 1 and the content of document D2.

As the applicant has already stated in the description, the present invention aims to improve the Maurer test or the universal test described in D2.

In particular, the invention consists in replacing step 4 of the universal test with the specific calculation of the function $c(L, K)$.

However, the present wording of independent method Claim 1 mentions only a "**calculation of the function $c(L,K)$** ", without giving any detail on how said calculation is carried out. In other words, the scope of the protection is not limited to a particular type of calculation and also comprises, for example, the calculation of D2. It is only in Claim 4 that the steps for calculating the function $c(L,K)$, according to the invention, are claimed. Consequently, the invention, as presently claimed in Claim 1, is considered to be already disclosed by document D2.

It is not deemed necessary at this stage of the proceedings to continue with the analysis of document D2, because the examiner's analysis corresponds with that of the applicant as given on page 4 of the description.

Therefore the subject matter of Claim 1 is not novel and Claim 1 does not fulfil the requirements of PCT Article 33(2).

2. Claim 4 should therefore be combined with independent method Claim 1 (see also Box VIII).

None of the documents cited envisages replacing step 4 of the universal test by a more specific calculation of the function $c(L,K)$ based on a probabilistic analysis of the universal test. This method enables the accuracy guaranteed by the theoretical analysis of the universal test to be achieved and, in particular, improves the security of portable smart card devices.

Such a solution involves an inventive step and

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 99/01996

Claim 4 therefore fulfils the requirements of PCT
Article 33(3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. To fulfil the requirements of PCT Rule 6.3(b) the claims should be **correctly** presented in the two-part form with the features known in combination from the prior art (see document D2, cited in Box V) appearing in the first part.
2. To fulfil the requirements of PCT Rule 5.1 (a)(iii), the introductory part of the description should be made consistent with the new claims proposed by the applicant.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. **Method Claim 1** is unclear in that it does not contain all the technical features essential for the definition of the invention as required by PCT Article 6 in combination with PCT Rule 6.3(b).

Claim 1 does not specify how the fourth step, i.e. the calculation of the function $c(L,K)$, is carried out.

However, this feature is essential, since, as the applicant has already recognised in the description, the method consists in replacing step 4 of the universal test with the specific calculation of the function $c(L,K)$ (see page 4 of the description).

This feature could be taken from dependent Claim 4.

- 2a. **Claim 7** should be considered to be an independent claim.

A claim can comprise a reference to another claim without being a dependent claim (cf. PCT Guidelines Ch. III, 3.7a).

In particular, a claim referring to a claim from another category (such as, for example, a device claim referring to a method claim) is, by definition, an independent claim (cf. PCT Guidelines same paragraph).

However, the fact that a device claim refers to a method claim merely means that the device is suitable for carrying out the method of said claim and does not define **the means** required for said

VIII. Certain observations on the international application

method (cf. also PCT Guidelines Ch. III, 4.8).

Claim 7 should explicitly contain, even if the reference to the method claim is retained, all the essential technical features needed for the definition of the invention (PCT Article 6 in combination with PCT Rule 6.3(b)) and should not attempt to replace them by a reference to the method claim.

An independent claim should be understandable *per se* without the need to refer to another claim.

- 2b. However, it appears to be important to note at this stage of the proceedings that the description does not describe any embodiments of a device and does not contain any figure describing such an embodiment.

Claim 7 uses, practically *expressis verbis*, the wording of the description and contains no additional detail.

Therefore it appears to be impossible to clarify the device claim using the structural features comprised in the description, since the description does not contain any structural features. Therefore, the application, concerning the device, does not appear to be disclosed in a sufficiently clear and complete manner for a person skilled in the art to be able to carry it out (PCT Article 5).

- 3a. The same objections relating to clarity that concern Claim 7 also apply to **Claim 10**. Said claim claims a device according to one of Claims 1-6. However, Claims 1-6 are not device claims, but method claims

VIII. Certain observations on the international application

(category problem). Does the applicant mean a device **for carrying out a method according to** Claims 1-6?

If this is the case, the applicant has not described any structural feature of such a device (the essential features are lacking). Furthermore, no structural features are described in the description, consequently, clarification appears impossible (PCT Article 5).

- 3b. Furthermore, two other problems of clarity are to be found in Claim 10. Firstly, Claim 10 refers to Claims 1-6 which do not contain any references to a portable device. Claim 10 mentions **said** portable devices. Secondly, the device is a **self**-verification device, verifying its own random number generator. If this **self**-checking device is already on a portable device, what does the external device verify? Once again, the description cannot give any further clarification since the claims restate, word for word, the little that is described in the description concerning said device.

4. In conclusion, in the light of the serious problems of clarity, it is suggested that all the device claims be deleted and that only the method claims be retained, combining the features of Claim 1 with those of Claim 4.

091763158

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

VERSION RÉVISÉE

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
24 février 2000 (24.02.2000)

PCT

(10) Numéro de publication internationale
WO 00/10284 A1(51) Classification internationale des brevets⁷: G06F 17/17(81) États désignés (*national*): AU, CA, CN, IN, JP, MX, SG, US.

(21) Numéro de la demande internationale:

PCT/FR99/01996

(84) États désignés (*régional*): brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(22) Date de dépôt international: 16 août 1999 (16.08.1999)

(25) Langue de dépôt: français

(26) Langue de publication: français

Publiée:

— Avec rapport de recherche internationale.
— Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.(30) Données relatives à la priorité:
98/10592 17 août 1998 (17.08.1998) FR(71) Déposant (*pour tous les États désignés sauf US*): GEM-PLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(88) Date de publication du rapport de recherche internationale révisé: 7 juin 2001

(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*): CORON, Jean-Sébastien [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR).(15) Renseignements relatifs à la correction:
voir la Gazette du PCT n° 23/2001 du 7 juin 2001, Section II

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

RECEIVED

JUL 02 2001

Technology Center 2100

(54) Title: METHOD FOR IMPROVING RANDOM TESTING

(54) Titre: PROCEDE D'AMELIORATION D'UN TEST STATISTIQUE

(57) Abstract: The invention concerns a method for testing sources generating random numbers, particularly sources set up in the context of cryptographic systems such as random number generators incorporated in chip cards. The invention is particularly designed to be used for testing and validating electronic devices such as chip cards, PCMCIA, badges, contactless cards or any other similar portable apparatus.

(57) Abrégé: La présente invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce. Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.

WO 00/10284 A1

PCT/FR 99/01996

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/17

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

INSPEC, EPO-Internal, SCISEARCH

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CORON JS, NACCACHE D: "AN ACCURATE EVALUATION OF MAURER'S UNIVERSAL TEST" GEMPLUS' CORPORATE PRODUCT R&D DIVISION - TECHNICAL REPORT IT01-1998, 1998, pages 1-13, XP002101030 http://www.gemplus.fr/smart/r_d/publications/download/it01.pdf the whole document	1-10
A	MAURER U M: "A universal statistical test for random bit generators" JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, pages 89-105, XP002101031 ISSN 0933-2790 cited in the application page 101, line 4 - line 7 -/--	1-10

RECEIVED
JUL 02 2001
Technology Center 2100

☒ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

22 March 2001

Date of mailing of the international search report

28/03/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Pierfederici, A

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>SADEGHIYAN B ET AL: "A new universal test for bit strings" INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, WOLLONGONG, NSW, AUSTRALIA, 24-26 JUNE 1996, pages 311-319, XP002101032 ISBN 3-540-61991-7, 1996, Berlin, Germany, Springer-Verlag, Germany</p>	
A	<p>DALLE MOLLE J W ET AL: "Higher-order cumulant spectral-based statistical tests of pseudo-random variate generators" 1992 WINTER SIMULATION CONFERENCE PROCEEDINGS (CAT. NO.92CH3202-9), ARLINGTON, VA, USA, 13-16 DEC. 1992, pages 618-625, XP002101033 ISBN 0-7803-0798-4, 1992, New York, NY, USA, IEEE, USA</p>	

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F17/17

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

INSPEC, EPO-Internal, SCISEARCH

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CORON JS, NACCACHE D: "AN ACCURATE EVALUATION OF MAURER'S UNIVERSAL TEST" GEMPLUS' CORPORATE PRODUCT R&D DIVISION - TECHNICAL REPORT IT01-1998, 1998, pages 1-13, XP002101030 http://www.gemplus.fr/smart/r_d/publications/download/it01.pdf le document en entier	1-10
A	MAURER U M: "A universal statistical test for random bit generators" JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, pages 89-105, XP002101031 ISSN 0933-2790 cité dans la demande page 101, ligne 4 - ligne 7	1-10

-/--

☒ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

22 mars 2001

Date d'expédition du présent rapport de recherche internationale

28/03/2001

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Fonctionnaire autorisé

Pierfederici, A

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>SADEGHIYAN B ET AL: "A new universal test for bit strings" INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, WOLLONGONG, NSW, AUSTRALIA, 24-26 JUNE 1996, pages 311-319, XP002101032 ISBN 3-540-61991-7, 1996, Berlin, Germany, Springer-Verlag, Germany</p> <p>-----</p> <p>A DALLE MOLLE J W ET AL: "Higher-order cumulant spectral-based statistical tests of pseudo-random variate generators" 1992 WINTER SIMULATION CONFERENCE PROCEEDINGS (CAT. NO.92CH3202-9), ARLINGTON, VA, USA, 13-16 DEC. 1992, pages 618-625, XP002101033 ISBN 0-7803-0798-4, 1992, New York, NY, USA, IEEE, USA</p> <p>-----</p>	



DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : H04L 9/22	A1	(11) Numéro de publication internationale: WO 00/10284 (43) Date de publication internationale: 24 février 2000 (24.02.00)
(21) Numéro de la demande internationale: PCT/FR99/01996 (22) Date de dépôt international: 16 août 1999 (16.08.99) (30) Données relatives à la priorité: 98/10592 17 août 1998 (17.08.98) FR (71) Déposant (pour tous les Etats désignés sauf US): GEM-PLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): CORON, Jean-Sébastien [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).		(81) Etats désignés: AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Avec rapport de recherche internationale.</i>
(54) Title: METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD (54) Titre: PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE ET DISPOSITIFS ELECTRONIQUES COMPRENANT CE PROCEDE (57) Abstract <p>The invention concerns a method for testing sources generating random numbers, particularly sources set up in the context of cryptographic systems such as random number generators incorporated in chip cards. The invention is particularly designed to be used for testing and validating electronic devices such as chip cards, PCMCIA, badges, contactless cards or any other similar portable apparatus.</p> (57) Abrégé <p>La présente invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce. Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.</p>		

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	B Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Biélorus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE
ET DISPOSITIFS ELECTRONIQUES COMPRENANT CE
PROCEDE**

5 L'invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

Elle est particulièrement destinée à être mise en oeuvre dans le
10 test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.

La plupart des systèmes de cryptographie à clé publique (dite aussi cryptographie asymétrique) et clé secrète (dite aussi cryptographie
15 symétrique) nécessitent le tirage d'aléas secrets. Il est primordial que de tels aléas, ou nombres, destinés à servir comme clés ultérieurement, soient à priori imprévisibles et ne présentent pas de régularités permettant de les retrouver par des stratégies de recherche exhaustive ou exhaustive améliorée pour laquelle les clés les plus probables sont cherchées en
20 premier lieu.

A ce titre, il existe plusieurs procédés permettant de tester les aléas générés par une source aléatoire et de s'assurer que ladite source fonctionne correctement et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une
25 altération par des radiations induites.

Chacun de ces procédés s'applique à une suite, appelée aussi séquence, de nombres entiers compris entre 0 et une valeur d, ladite suite étant générée par la source aléatoire.

Le procédé de test le plus connu est le test dit de "fréquence". Il
30 s'agit de compter le nombre d'apparitions de chaque entier compris entre 0 et une valeur d dans ladite séquence. Le nombre d'apparitions de chaque entier est ensuite évalué statistiquement.

Un second procédé de test dit de "séries" consiste en un comptage et une évaluation statistique du nombre d'apparitions de tous
35 les couples possibles d'entiers compris entre 0 et une valeur d. Ce

COPIE DE CONFIRMATION

procédé de test peut être généralisé au comptage des triplets, quadruplets d'entiers, etc...

Un troisième procédé de test dit de "trou" existe. Un trou dans une séquence est une suite de nombres à l'extérieur d'un intervalle prédéterminé. Il s'agit d'une évaluation statistique de la longueur desdits trous dans la séquence.

Un quatrième procédé de test, dit test du "poker", existe. Le test consiste à grouper les nombres de la séquence par groupe de cinq nombres et à compter dans chaque quintuplet combien de valeurs différentes apparaissent.

Un cinquième procédé de test dit de "collecte de coupons" consiste à évaluer statistiquement la taille de séquence nécessaire pour que toutes les valeurs entières comprises entre 0 et d apparaissent dans ladite séquence.

Le détail de ces procédés se trouve dans l'ouvrage intitulé: "Knuth, The art of computer programming, vol. 2, Seminumerical algorithms".

Un autre procédé de test populaire est le test universel de Maurer décrit dans l'ouvrage "Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105". Ce test présente l'avantage de révéler tous les défauts décelables par les procédés de tests précédemment cités ainsi que d'autres défauts statistiques non détectés par ces mêmes procédés de test.

Le procédé de test, dit de Maurer, également dénommé universel, comprend les étapes suivantes:

Première étape: Génération d'une séquence de $(Q+K)*L$ bits par la source aléatoire. Q, K et L sont des paramètres d'entrée. Les bits de la séquence sont groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K. La longueur est mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.

Deuxième étape: Calcul du paramètre du test, noté fTU; cette deuxième étape comprenant les étapes suivantes, appelées sous-étapes 2.1 à 2.5 :

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L ;

2.2 Pour n variant de 1 à Q, faire le calcul: $\text{tab}[\text{block}[n]]=n$;

2.3 Initialiser le nombre Sum à 0;

2.4 Pour n variant de $Q+1$ à $Q+K$, exécuter le calcul :

Ajouter $\log(n - \text{tab}[\text{block}[n]])$ à Sum ;

Faire le calcul: $\text{tab}[\text{block}[n]] = n$;

2.5 Le paramètre fTU du test est donné par:

$$\text{fTU} = (\text{Sum}/K) / \log(2);$$

Troisième étape: Calcul de la variance par block de paramètre du test, notée Var . Son expression précise est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105 ", qui est :

$$\text{Var} = (1-z) \sum_{i=1}^{\infty} \log_2(i)^2 \cdot z^{i-1} - ((1-z) \sum_{i=1}^{\infty} \log_2(i) \cdot z^{i-1})^2,$$

avec $\log_2(z) = \log(z)/\log(2)$ et $z = 1 - 2^{-L}$

Quatrième étape: Calcul de la fonction $c(L, K)$. Une expression
15 approchée de cette fonction est donnée dans l'article de l'ouvrage précédent, qui est:

$$c(L, K) = 0,7 - 0,8/L + (1,6 + 12,8/L) \cdot K^{(-4/L)};$$

Cinquième étape: Calcul de l'écart type du paramètre de test,
noté σ : $\sigma = c(L, K) \cdot \sqrt{(\text{Var}/K)}$;

20 Sixième étape: Calcul du paramètre y ; y est déterminé à partir du taux de rejet du test fixé en entrée, noté p . y doit vérifier l'équation:

$$N(-y) = p.$$

N est la fonction de densité normale décrite dans l'ouvrage " R. Langley, Practical statistics, Dover publications, New-York, 1968 ".

25 L'équation $N(-y) = p$ peut être résolue en utilisant une table de valeurs de N . Une telle table est fournie dans l'article précédent;

Septième étape: Calcul de la valeur moyenne idéale du test, notée $E[\text{fTU}]$. Son expression est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n°2, 1992, pp. 89-105 ", et

30 vaut :

$$E[\text{fTU}] = (1-z) \sum_{i=1}^{\infty} \log_2(i) \cdot z^{i-1}$$

avec $\log_2(z) = \log(z)/\log(2)$ et $z = 1 - 2^{-L}$

Huitième étape: Calcul des bornes t_1 et t_2 . Elles sont données par l'équation: $t_1 = E[fTU] - y \cdot \sigma$ et $t_2 = E[fTU] + y \cdot \sigma$;

Neuvième étape: Résultat du test:

5 Si le paramètre du test fTU est compris entre t_1 et t_2 , alors le générateur de nombre aléatoire est accepté. Dans le cas contraire, il est refusé.

10 Le procédé de test universel est donc basé sur une approximation dans le calcul de la fonction $c(L, K)$. Cette approximation rend le test moins précis que ce que veut la garantie théorique lui servant de base. Il est possible de montrer que dans certains cas, le test universel s'avère 2,67 fois trop permissif par rapport à ce que permet la théorie.

15 La présente invention a pour objet un procédé de test amélioré permettant d'atteindre la précision réelle garantie par l'analyse théorique du test universel. Ce test sert notamment à améliorer la sécurité de dispositifs portables du type carte à puce.

20 Le procédé de l'invention consiste à remplacer l'étape 4 du test universel par le calcul précis de la fonction $c(L, K)$. Ce calcul est basé sur une analyse probabiliste du test universel.

La présente invention donne trois expressions distinctes de la fonction $c(L, K)$, suivant les valeurs des paramètres L et K .

25 La première expression de $c(L, K)$ est valable quelque soient les paramètres L et K .

La deuxième expression de $c(L, K)$ est valable dans le cas où la valeur L est comprise entre 3 et 16 et la valeur K est supérieur à $30 \cdot 2^L$, ce qui correspond au cas le plus usuel d'utilisation du test. Elle est beaucoup plus simple à calculer que la première expression et peut donc s'effectuer
30 à bord d'un simple micro-contrôleur en quelques millisecondes.

La troisième expression de $c(L, K)$ est valable pour une valeur de $L > 16$ et une valeur de $K > 30 \cdot 2^L$. Cette expression est encore plus simple à calculer.

La première expression de $c(L,K)$ peut s'obtenir par le procédé décrit ci-dessous qui comporte neuf étapes:

1. Calculs de: $u=1-2^{-L}$ et $v=1-1/(2^L-1)$;
u et v étant des nombres réels;
2. Création de deux tableaux tab1 et tab2 de dimension $60 \cdot 2^L$;
3. Remplissage des tab1 et tab2: pour cela,
 - 3.1 Exécuter $z=u$, $\text{sum}=0$, $z1=1$;
 - 3.2 Pour i allant de 1 à $30 \cdot 2^L$, répéter les deux opérations qui sont: ajouter $\log_2(i) \cdot z1$ à sum, dans laquelle \log_2 désigne le logarithme en base 2, et
calculer: $z1=z1 \cdot z$;
 - 3.3 Exécuter $\text{tab1}[0]=(1-z) \cdot \text{sum}$;
 - 3.4 Pour i allant de 1 à $60 \cdot 2^L$,
Exécuter $\text{tab1}[i]=(\text{tab1}[i-1]-(1-z) \cdot \log_2(i))/z$;
 - 3.5 Répéter les étapes 3.1, 3.2, 3.3, 3.4 en remplaçant u par v et tab1 par tab2;
4. Calcul de la variance par bloc notée Var;
 - 4.1 Exécuter $\text{sum}=0$ et $x=1$;
 - 4.2 Pour i variant de 1 à $30 \cdot 2^L$, exécuter les deux opérations qui sont:
Ajouter $\log_2(i)^2 \cdot x$ à sum et
Exécuter $x=x \cdot z$;
 - 4.3 Faire $\text{Var}=\text{sum}/2^L - \text{tab1}[0]^2$;
5. Calcul de $P(K)$:
 - 5.1 Faire $\text{sum}=0$ et $x=1$
 - 5.2 Pour i variant de 1 à $30 \cdot 2^L$: faire les trois opérations suivantes:
Calculer y: $y=u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot (\text{tab2}[0] - v^i \cdot \text{tab2}[i]) + u \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K-1])$,
Ajouter $y \cdot x$ à sum,
Exécuter $x=x \cdot u$;
 - 5.3 Exécuter $P(K)=u^{(K-1)} \cdot \text{sum}$;

6. Calcul de $P(1)$:Même procédé qu'à l'étape 5 en remplaçant K par 1;7. Calcul de $Q(K)$:7.1 Faire $\text{sum}=0$, $\text{sum2}=0$ et $x=1$,5 7.2 Pour i variant de 1 à $30 \cdot 2^L$:Ajouter $i \cdot \log_2(i) \cdot u^{(i-2)}$ à sum2 ;

Exécuter les trois opérations suivantes:

calculer $y = u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot ((i+K) \cdot \text{tab2}[0] -$ $v_i \cdot \text{tab2}[i]) - 2^{(-L)} \cdot \text{sum2} + u \cdot (i+K-1) \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] -$ 10 $\text{tab2}[i+K-1])$,Ajouter $y \cdot x$ à sum ,Exécuter $x = x \cdot u$;7.3 Exécuter $Q(K) = u^{(K-1)} \cdot \text{sum}$ 8. Calcul de $Q(1)$ 15 Même procédé qu'à l'étape 7 en remplaçant K par 19. Calcul de $c(L, K)$

$$c(L, K) = \sqrt{(1 - 2/\text{Var}^*(P(1) - P(K) - (Q(1) - Q(K))/K)}$$

La deuxième expression de $c(L, K)$ est valable pour $K > 30 \cdot 2^L$.

20 Elle se calcule d'après le procédé suivant en deux étapes:

Première étape: Lecture des valeurs de $e(L)$ et $d(L)$, e et d étant des réels, listées dans le tableau suivant, pour L compris entre 3 et 16:

	L	$d(L)$	$e(L)$
25	3	0, 2732725	0,4890883
	4	0,3045101	0,4435381
	5	0,3296587	0,4137196
	6	0,3489769	0,3941338
	7	0,3631815	0,3813210
30	8	0, 3732189	0,3730195
	9	0,3800637	0,3677118
	10	0,3845867	0,3643695
	11	0,3874942	0,3622979
	12	0,3893189	0,3610336
35	13	0,3904405	0,3602731

14	0,3911178	0,3598216
15	0,3915202	0,3595571
16	0,3917561	0,3594040

5 Deuxième étape: Calcul de la valeur $c(L,K)$ à l'aide de la formule:

$$c(L,K)=\sqrt{(d(L)+e(L)*2^L/K)}$$

La troisième expression de $c(L,K)$ est valable pour $L>16$ et
 $K>30*2^L$. Elle est donnée par la formule suivante:

10
$$c(L,K)=\sqrt{(1-6/\pi^2+2/\pi^2*(4*\log(2)-1)*2^L/K)}$$

La présente invention concerne également, comme cela a été dit
au début de la description, page une, un dispositif électronique non
représenté par une figure ou un schéma. Ce dispositif électronique est un
15 dispositif d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-
vérifiant et contrôlant l'intégrité de son générateur aléatoire à partir des
trois variantes du procédé de l'invention, décrits également ci-dessus, ou
plus explicitement à partir des trois expressions distinctes de la fonction
 $c(L, K)$, ceci afin de s'assurer que ledit générateur fonctionne
20 correctement en général et ne présente pas de dérive suite à des
changements de paramètres externes d'origine malveillante telle qu'une
altération par des radiations induites en particulier.

De manière préférentielle, le dispositif électronique effectuant le
25 test est un dispositif portable, plus particulièrement il consiste, par
exemple, en une carte à puce, une carte sans contact, une carte
PCMCIA, un badge, une montre intelligente.

Enfin, le dispositif électronique de l'invention peut être un
30 dispositif extérieur constitué d'une machine ou installation destinée à
tester le bon fonctionnement de générateurs aléatoires embarqués à bord
desdits dispositifs portables. Ce dispositif extérieur permet un échange
d'informations avec le dispositif portable de manière à vérifier que le
générateur aléatoire fonctionne correctement. Le dispositif extérieur inter-

agit avec le dispositif portable pour vérifier l'intégrité de son générateur aléatoire.

REVENDECATIONS

1. Procédé de test de source de nombre aléatoire comprenant les étapes suivantes:

5 Première étape: Génération d'une séquence de $(Q+K)*L$ bits par la source aléatoire, Q, K et L étant des paramètres d'entrée. Les bits de la séquence étant groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K, la longueur étant mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.

10 Deuxième étape: Calcul du paramètre du test, noté fTU; cette deuxième étape comprenant les étapes suivantes, appelées sous-étapes 2.1 à 2.5 :

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L ;

2.2 Pour n variant de 1 à Q, faire le calcul: tab[block[n]]=n;

15 2.3 Initialiser le nombre Sum à 0;

2.4 Pour n variant de Q+1 à Q+K, exécuter le calcul en deux opérations:

Ajouter $\log(n-\text{tab}[\text{block}[n]])$ à Sum;

Exécuter le calcul: tab[block[n]]=n;

20 2.5 Le paramètre fTU du test est donné par:

$\text{fTU} = (\text{Sum}/K)/\text{Log}(2)$;

Troisième étape: Calcul de la variance par block de paramètre du test, notée Var, à partir de l' expression suivante:

$$25 \quad \text{Var} = (1-z) \sum_{i=1}^{\infty} \log_2(i)^2 \cdot z^{i-1} - ((1-z) \sum_{i=1}^{\infty} \log_2(i) \cdot z^{i-1})^2,$$

avec $\log_2(z) = \log(z)/\log(2)$ et $z = 1 - 2^{-L}$

Quatrième étape: Calcul de la fonction c(L,K);

Cinquième étape: Calcul de l'écart type du paramètre de test,

30 noté σ : $\sigma = c(L,K) \cdot \sqrt{(\text{Var}/K)}$;

Sixième étape: Calcul du paramètre y; y est déterminé à partir du taux de rejet du test fixé en entrée, noté ρ . y doit vérifier l'équation:

$N(-y) = \rho$.

N est la fonction de densité normale

Septième étape: Calcul de la valeur moyenne idéale du test, notée $E[fTU]$, donnée par la formule suivante.

$$E[fTU] = (1-z) \sum_{i=1}^{\infty} \log_2(i) 2^{z^i - 1}$$

avec $\log_2(z) = \log(z)/\log(2)$ et $z = 1 - 2^{-L}$

Huitième étape: Calcul des bornes t_1 et t_2 . Elles sont données par l'équation: $t_1 = E[fTU] - y \cdot \sigma$ et $t_2 = E[fTU] + y \cdot \sigma$;

Neuvième étape: Résultat du test : le générateur de nombre aléatoire étant accepté si le paramètre du test fTU est compris entre t_1 et t_2 , et rejeté dans le cas contraire,

Ledit procédé étant caractérisé en ce que la quatrième étape consiste en un calcul de la fonction $c(L, K)$ valable quelques soient les paramètres L et K .

2. Procédé de test de source de nombre aléatoire selon la revendication 1 caractérisé en ce que la quatrième étape consiste en un calcul de la fonction $c(L, K)$ valable dans le cas où la valeur de L est compris entre 3 et 16 et la valeur de K est supérieur à $30 \cdot 2^L$.

3. Procédé de test de source de nombre aléatoire selon la revendication 1 caractérisé en ce que la quatrième étape consiste en un calcul de la fonction $c(L, K)$ valable pour une valeur de $L > 16$ et une valeur de $K > 30 \cdot 2^L$.

4. Procédé selon la revendication 1 caractérisé en ce que le calcul de la fonction $c(L, K)$ comporte neuf étapes:

1. Calcul de: $u = 1 - 2^{-L}$ et $v = 1 - 1/(2^L - 1)$;

u et v étant des entiers réels;

2. Création de deux tableaux tab_1 et tab_2 de dimension $60 \cdot 2^L$;

- 3.1 Exécuter $z=u$, $sum=0$, $z1=1$;
- 3.2 Pour i allant de 1 à $30 \cdot 2^L$, répéter les deux opérations qui sont: ajouter $\log_2(i) \cdot z1$ à sum , dans laquelle \log_2 désigne le logarithme en base 2, et
- 5 calculer: $z1=z1 \cdot z$;
- 3.3 Exécuter $tab1[0]=(1-z) \cdot sum$
- 3.4 Pour i allant de 1 à $60 \cdot 2^L$,
Exécuter $tab1[i]=(tab1[i-1]-(1-z) \cdot \log_2(i))/z$
- 3.5 Répéter les étapes 3.1, 3.2, 3.3, 3.4 en remplaçant u par v et
- 10 $tab1$ par $tab2$;
4. Calcul de la variance par bloc notée Var ;
- 4.1 Exécuter $sum=0$ et $x=1$;
- 4.2 Pour i variant de 1 à $30 \cdot 2^L$, exécuter les deux opérations qui sont:
- 15 Ajouter $\log_2(i)^2 \cdot x$ à sum et
Exécuter $x=x \cdot z$
- 4.3 Faire $Var=sum/2^L-tab1[0]^2$;
5. Calcul de $P(K)$:
- 5.1 Faire $sum=0$ et $x=1$;
- 20 5.2 Pour i variant de 1 à $30 \cdot 2^L$: faire les trois opérations suivantes:
Calcul de $y: y=u^2 \cdot (tab2[i+K-1]-tab1[i+K]) \cdot (tab2[0]-v^i \cdot tab2[i])+u \cdot tab1[0] \cdot (tab1[i+K-1]-tab2[i+K-1])$,
Ajouter $y \cdot x$ à sum ,
- 25 Exécuter $x=x \cdot u$;
- 5.3 Exécuter $P(K)=u^{(K-1)} \cdot sum$;
6. Calcul de $P(1)$:
Même procédé qu'à l'étape 5 en remplaçant K par 1;
7. Calcul de $Q(K)$:
- 30 7.1 Faire $sum=0$, $sum2=0$ et $x=1$,
- 7.2 Pour i variant de 1 à $30 \cdot 2^L$:
Ajouter $i \cdot \log_2(i) \cdot u^{(i-2)}$ à $sum2$;
Exécuter les trois opérations suivantes:

calculer $y = u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot ((i+k) \cdot \text{tab2}[0] - v_i \cdot \text{tab2}[i]) - 2 \cdot (-L) \cdot \text{sum2} + u \cdot (i+K-1) \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K-1])$,
Ajouter $y \cdot x$ à sum,
5 Exécuter $x = x \cdot u$;
7.3 Exécuter $Q(K) = u^{(K-1)} \cdot \text{sum}$
8. Calcul de $Q(1)$
Même procédé qu'à l'étape 7 en remplaçant K par 1
9. Calcul de $c(L, K)$
10 $c(L, K) = \sqrt{(1 - 2/\text{Var} \cdot (P(1) - P(K) - (Q(1) - Q(K))/K))}$

5. Procédé selon la revendication 2 caractérisé en ce que la
15 fonction $c(L, K)$ comporte deux étapes:

Première étape: Lecture des valeurs de $e(L)$ et $d(L)$, e et d étant des réels, listées dans le tableau suivant, pour L compris entre 3 et 16:

	L	d(L)	e(L)
20	3	0, 2732725	0,4890883
	4	0,3045101	0,4435381
	5	0,3296587	0,4137196
	6	0,3489769	0,3941338
	7	0,3631815	0,3813210
25	8	0, 3732189	0,3730195
	9	0,3800637	0,3677118
	10	0,3845867	0,3643695
	11	0,3874942	0,3622979
	12	0,3893189	0,3610336
30	13	0,3904405	0,3602731
	14	0,3911178	0,3598216
	15	0,3915202	0,3595571
	16	0,3917561	0,3594040

35 Deuxième étape: Calcul de la valeur $c(L, K)$ à l'aide de la formule:

$$c(L,K)=\sqrt{(d(L)+e(L)*2^L/K)}$$

6. Procédé selon la revendication 3 caractérisé en ce que le calcul de la fonction $c(L,K)$ est réalisée par la formule suivante:

5
$$c(L,K)=\sqrt{(1-6/\pi^2+2/\pi^2*(4*\log(2)-1)*2^L/K)}$$

7. Dispositif électronique d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-vérifiant et contrôlant l'intégrité de son générateur aléatoire, afin de s'assurer que ce dernier fonctionne
10 correctement en général et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites en particulier, selon l'une quelconque des revendications 1 à 3.

15 8. Dispositif électronique selon la revendication 7 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

9. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est une carte à puce, une carte sans contact, une carte
20 PCMCIA, un badge, une montre intelligente.

10. Dispositif électronique selon l'une quelconque des revendications 1 à 6 caractérisé en ce qu'un dispositif extérieur effectuant le test est constitué d'une machine ou installation destinée à tester le bon
25 fonctionnement de générateurs aléatoires embarqués à bord desdits dispositifs portables.

30

35

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/FR 99/01996

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SADEGHIYAN B ET AL: "A new universal test for bit strings" LECTURE NOTES IN COMPUTER SCIENCE, US, SPRINGER VERLAG, NEW YORK, NY, page 311-319-319 XP002101032 ISSN: 0302-9743 abstract page 311, line 1 -page 318, line 10	1-9
A	MAURER U M: "A universal statistical test for random bit generators." J.CRYPTOL. (USA), JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, 1992, pages 89-105, XP002122895 cited by the applicant	1-9

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

17 November 1999

Date of mailing of the international search report

30/11/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3018

Authorized officer

Gautier, L

RAPPORT DE RECHERCHE INTERNATIONALE

Je Internationale No

PCT/FR 99/01996

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/22

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L H03K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	SADEGHIYAN B ET AL: "A new universal test for bit strings" LECTURE NOTES IN COMPUTER SCIENCE, US, SPRINGER VERLAG, NEW YORK, NY, page 311-319-319 XP002101032 ISSN: 0302-9743 abrégé page 311, ligne 1 -page 318, ligne 10	1-9
A	MAURER U M: "A universal statistical test for random bit generators." J.CRYPTOL. (USA), JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, 1992, pages 89-105, XP002122895 cited by the applicant	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

17 novembre 1999

Date d'expédition du présent rapport de recherche internationale

30/11/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentkan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Fonctionnaire autorisé

Gautier, L